UN PLAN DE CYBERSÉCURITÉ POUR LA SOCIÉTÉ CIVILE : LES ENJEUX

Alex Comninos

INTRODUCTION

La sécurité des réseaux numériques et de l'information numérique en réseau revêt une importance croissante pour les pouvoirs publics, le secteur privé et la société civile. La cybercriminalité gagne en sophistication[1]. Les États s'accusent mutuellement de piratage[2]. Les organisations de la société civile, les États, les sociétés et les internautes sont exposés et deviennent les victimes de virus et de logiciels malveillants, de violations de données, de violations de la vie privée en ligne et de surveillance. Les gouvernements et les sociétés espionnent les citoyens, les défenseurs des droits humains (DDH) sont plus particulièrement victimes de cette surveillance. Le cyberactivisme devient une forme de protestation, souvent pour défendre les droits humains, mais il peut également porter atteinte aux droits ou déclencher des réactions des autorités qui portent atteinte à ces droits[3].

1. RSA 2012 Cybercrime Trends Report: The Current State of Cybercrime and What to Expect in 2012, http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf
2. Les États-Unis et la Chine s'accusent mutuellement d'attaques cybernétiques, RT (Russia Today), 19 février 2013, http://rt.com/usa/cyber-china-war-unit-604/
3. James Ball "By criminalising online dissent we put democracy in peril" The Guardian 1 August 2011, guardian.co.uk/commentisfree/2011/aug/01/onlinedissent-democracy-hacking; Cory Doctorow, Pirate Bay to Anonymous: DDoS is censorship, cut it out, BoingBoing, 1er mai 2012, http://boingboing.net/2012/05/11/pirate-bay-to-anonymous-ddos.html, Jay Leiderman, Justice for the PayPal WikiLeaks protesters: why DDoS is free speech, The Guardian, 22 janvier 2013, http://www.guardian.co.uk/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech

Alex Comninos est candidat au doctorat, Université Justus-Liebig, Giessen.

APC ASSOCIATION POUR LE PROGRÈS DES COMMUNICATIONS

Les femmes défenseurs des droits humains (FDDH), qui sont des parties prenantes importantes de la cybersécurité, sont vulnérables à la surveillance, à la sécurité de l'information et à des compromis dans la sécurité de l'information susceptibles de mettre leur vie en danger. En revanche, elles peuvent utiliser les TIC pour rendre compte et se défendre contre les violations des droits humains, ce qui doit être garanti[4].

Les gouvernements prennent prétexte de la sécurité nationale pour justifier la censure, le contrôle ou la surveillance de l'utilisation de l'internet et, parfois, pour faire cesser les communications. Certains militaires créent des cyber-unités, et on voit émerger une course aux armements dans le cyberespace[5], qui s'accompagne d'une croissance du « complexe cyber-industriel ». Le secteur privé participe de plus en plus au contrôle de l'internet. Par des mécanismes de responsabilité intermédiaire, les entreprises de télécommunication, les fournisseurs de services internet (FSI) et d'autres acteurs du secteur privé font la police sur l'internet[6].

Alors que les gouvernements, les militaires, les services de renseignement et le secteur privé prennent l'initiative des débats et des politiques sur la cybersécurité, la société civile doit assumer son rôle sur un pied d'égalité. Robert Deibert a fait valoir que la société civile « est de plus en plus reconnue comme une partie prenante importante de la gouvernance du cyberespace » et doit formuler une stratégie de cybersécurité « qui traite des menaces très réelles qui empoisonnent les gouvernements et les entreprises et qui aborde franchement les préoccupations nationales tout en protégeant et en préservant les réseaux ouverts d'information et de communication »[7].

Ce document présente quelques idées fortes en matière de cybersécurité, analyse certaines menaces importantes liées à la cybersécurité et offre des suggestions sur ce que devrait être l'approche de la société civile à l'égard de la cybersécurité.

4. Danna Ingleton, Let's stop our fear of tech leading to misuse of security legislation, in Crossing borders : cyberspace and national security, GenderIT, 25 octobre 2012, http://www.genderit.org/node/3684.

5. Ron Deibert, Towards a cyber security strategy for civil society, dans Alan Finlay (éd.) *Global Information Society Watch 2011: Internet rights and democratization,* APC & HIVOS, http://www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society.

6. Ibid.

7. Ibid.

CONCEPTUALISATION DE LA CYBERSÉCURITÉ

Définition

La cybersécurité désigne la sécurité des informations numériques stockées sur des réseaux électroniques, ainsi que la sécurité des réseaux qui stockent et transmettent l'information. Mais la définition du terme est loin de faire l'unanimité. *Cybersécurité* est parfois utilisé comme synonyme de *sécurité de l'information* – « la protection de l'information et des systèmes d'information contre un accès, une utilisation, une perturbation, une modification ou une destruction non autorisées afin d'en assurer la confidentialité, l'intégrité et la disponibilité »[8]. La sécurité de l'information et la cybersécurité renvoient généralement à la même chose. Toutefois, le terme sécurité de l'information est plutôt utilisé par les organisations et les professionnels des TI, alors que l'on parle plutôt de cybersécurité dans les débats sur les politiques et lorsque la sécurité de l'information est considérée comme une question de sécurité nationale.

L'Union internationale des télécommunications (UIT) définit la cybersécurité ainsi :

> « l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations et des utilisateurs[9] … La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber-environnement. Les objectifs généraux en matière de sécurité sont les suivants:

8. Intégrité « signifie protéger contre les modifications ou destructions inappropriées et englobe la non-répudiation et l'authenticité de l'information »; confidentialité « signifie préserver les restrictions autorisées à l'accès et à la divulgation, y compris les moyens de protéger la vie privée et l'information exclusive » et disponibilité « signifie assurer l'accès rapide et fiable à l'information et son utilisation ». Richard Kissel, *Glossary of Key Information Security Terms,* National Institute of Science and Technology, US Department of Commerce, février 2011, p. 93, http://books.google.com/books?id=k5H3NsBXIsMC

9. "Les actifs des organisations et des utilisateurs comprennent les appareils informatiques connectés, le personnel, les infrastructures, les applications, les services, les systèmes de télécommunication et la totalité de l'information transmise et stockée dans le cyber-environnement ».

Disponibilité; Intégrité, qui peut englober l'authenticité et la non-répudiation [et] Confidentialité »[10].

Cette définition est un peu plus large que celle de la sécurité de l'information. Au lieu de protéger uniquement les systèmes d'information, elle protège également « le cyber-environnement » (un terme plutôt vague) et les « actifs des utilisateurs ». Elle concerne non seulement la *protection des systèmes d'information*, mais aussi *l'utilisation des systèmes d'information pour protéger les actifs.*

Quelle devrait donc être la portée du concept de cybersécurité? Quels aspects devraient être inclus et lesquels devraient être exclus? Un rapport de l'OCDE[11] mentionne que la cybersécurité « en est arrivé à désigner beaucoup de choses. Cela conduit non seulement à des pouvoirs dont la portée et l'application sont beaucoup trop vastes, mais également au risque de réaliser un consensus illusoire »[12]. En incluant trop d'éléments, on risque de faire perdre sa cohérence au concept. Plus le concept de cybersécurité est large, plus il place de questions sous la houlette des agences militaires et de renseignement des États. Bien des questions, même si leur traitement dépend de l'utilisation sécurisée des technologies de l'information et de la communication (TIC) et de l'internet, ne sont pas nécessairement résolues au mieux au niveau de la sécurité nationale ou même des structures de la sécurité de l'information ou par des solutions étatiques ou militaires. Il n'est pas toujours utile de tout régler par la cybersécurité, même si elle comporte des dimensions évidentes de sécurité de l'information.

Titrisation

Lorsque les questions sont traitées comme des questions de sécurité, on leur donne une certaine urgence et importance. Parler d'une question comme d'un problème de sécurité implique souvent qu'elle présente une menace pour le mode de vie d'une société et justifie des mesures exceptionnelles ou d'urgence pour contrer la menace. Lorsque des questions sont transformées, en en faisant des questions de sécurité nationale, c'est ce qu'on appelle la titrisation. La titrisation consiste à « désigner une menace existentielle nécessitant une intervention d'urgence, ou des mesures spéciales, et l'acceptation par un public important de cette délégation spécifique»[13]. Lorsque les questions sont bien titrisées, elles deviennent des questions de sécurité nationale et leur traitement est modifié « au-delà des règles du jeu ». La question est considérée « comme un type particulier de politique ou comme quelque chose qui est au-dessus de la politique »[14]. La titrisation réussie comprend trois volets : la présentation d'une question comme une menace, la mesure d'urgence pour la contrer et les effets sur les relations entre les parties prenantes en changeant la façon dont la question est normalement traitée[15].

La titrisation du cyberespace est un facteur important qui façonne l'écosystème mondial des communications. Les questions relatives à la sécurité de l'information, à l'internet, à la gouvernance de l'internet et à d'autres domaines sont, à travers le prisme de la cybersécurité, titrisées et transformées en questions de sécurité nationale, ce qui a un effet négatif sur les structures de gouvernance et sur les mécanismes décisionnels existants liés à ces questions. La titrisation ne donne pas nécessairement une voix et un rôle plus importants à la société civile en tant que partie prenante dans la gouvernance de la question. Lorsque des mesures extraordinaires ou d'urgence s'imposent, nous devons faire en sorte que ces mesures n'aient pas de conséquences négatives sur la transparence et la sécurité de l'internet et n'aient pas de conséquences négatives sur les droits humains.

10. Union internationale des télécommunications, Telecommunications Standardization Sector, Overview of Cybersecurity, Recommandation UIT-T X.1205 (04/2008), http://www.itu.int/ITU-T/recommendations/rec.aspx?id=9136; Adopté par l'IUT, Résolution 181, Guadalajara, 2010, http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf

11. Organisation de coopération et de développement économiques.

12. OCDE, "Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies", OCDE Digital Economy Papers, No. 212, OECD Publishing, 2012. http://dx.doi.org/10.1787/5k8zq92sx138-en, p 6.

13. Barry Buzan, Ole Waever, & Jaap de Wilde, 1998. *Security: a new framework for analysis. Lynne* Rienner: Boulder, Colorado, p. 27.

14. Ibid, p. 24.

15. Ibid.

Perspective historique : L'élargissement et l'approfondissement du concept de sécurité

L'histoire du concept de sécurité contient des leçons qui peuvent s'appliquer à la cybersécurité. Au cours des trois dernières décennies, le concept de sécurité, ainsi que les programmes de sécurité d'État se sont élargis pour inclure de nombreux secteurs et questions. Le contexte de la détente et de la fin de la Guerre froide a donné lieu à de nouveaux débats théoriques et politiques entre ceux qui militent pour l'élargissement de la définition de la sécurité et du programme de sécurité au-delà de la sécurité nationale et des questions stratégiques de la Guerre froide et ceux qui veulent conserver la définition étroite et le programme de sécurité, en se concentrant sur les questions militaires et de sécurité nationale. Depuis la fin de la Guerre froide, les gouvernements, les militaires, les milieux universitaires et la société civile ont participé à l'élargissement du concept de sécurité pour y inclure d'autres secteurs, qui ne sont pas traditionnellement liés à la sécurité nationale, par exemple, la sécurité culturelle, la sécurité économique, la sécurité environnementale, la sécurité climatique et la sécurité alimentaire. Parallèlement, le concept a été « approfondi » pour inclure l'humain comme objet central de la sécurité, plutôt que les États ou les militaires.

Le concept de sécurité postérieur à la Guerre froide est désormais « très large ... présente toujours le problème d'être très large », il est « encore plus abstrait qu'auparavant », est encore un concept qui « est entre les mains de l'État » et peut être utilisé contre des personnes16. Avec une définition large de la sécurité, les pouvoirs publics ont désormais davantage de prétextes pour déployer l'appareil coercitif de l'État ou pour appliquer des mesures exceptionnelles - comme la surveillance et la régulation d'un nombre croissant de questions. De nombreuses questions qui devraient relever de la société civile relèvent de la sécurité nationale et donnent souvent plus de pouvoir à l'État pour intervenir.

Le concept de cybersécurité fait actuellement l'objet d'un approfondissement et d'un élargissement similaires. La cybersécurité et la sécurité de l'information étaient auparavant des concepts techniques, principalement traités par les « technophiles », les professionnels, les entreprises, les États et les militaires et les agences de renseignement et de sécurité. Les concepts sont de plus en plus importants pour nous tous et se sont élargis au-delà des préoccupations étroites du milieu technique, des entreprises et de l'État. Les questions de cybersécurité peuvent donc faire intervenir davantage de parties prenantes. Toutefois, ce processus s'accompagne d'un élargissement du programme de la cybersécurité. Or, en raison de cet élargissement, d'autres aspects problématiques de la gouvernance de l'internet, de la gouvernance mondiale, de la gouvernance nationale, de la législation et de la réglementation relèvent des programmes de cybersécurité et de sécurité nationale des États. Ces problèmes sortent ainsi des structures de gouvernance actuelles où ils sont traités par des approches multipartites. La société civile risque donc d'être marginalisée. Par conséquent, elle doit veiller à pouvoir exploiter l'élargissement du concept de cybersécurité sans marginaliser son rôle d'acteur. Lorsque nous parlons de cybersécurité, ce qui est en jeu, c'est la voix et le pouvoir de la société civile en tant qu'acteur.

QUESTIONS À EXAMINER

Ce document n'a pas l'ambition de présenter un aperçu complet de toutes les menaces liées à la cybersécurité, son but est plutôt d'encourager une réflexion critique sur la cybersécurité et de soulever certaines questions pour aider la société civile à formuler des stratégies sur la cybersécurité. Quelques questions thématiques importantes sur la cybersécurité seront analysées ci-dessous, avant de passer aux recommandations.

Le discours techno et le discours alarmiste

La cybersécurité est une question plutôt complexe pour les internautes qui ne possèdent pas un bagage technique. Par conséquent, les médias, les décideurs, les parties prenantes des pouvoirs publics, des entreprises et de la société civile, entre autre, acceptent tel quel ce qu'on leur dit. Tout ce qui est lié à la cybersécurité peut être facilement mal interprété, mal compris, déformé ou comporter des erreurs. En raison de l'anonymat relatif sur l'internet, il est difficile d'attribuer la responsabilité ou la causalité des cyber-attaques et des incidents

16. Voir "A Conversation with Annette Seegers" et pour une explication plus longue, voir, Annette Seegers, "The New Security in a Democratic South Africa", presentation at The Robert Strauss Center for International Security and Law", 1er novembre 2010, http://blip.tv/robert-strauss-center/the-new-security-in-democratic-south-africa-4362239. Based on this paper Seegers, Annette (2010) 'The new security in democratic South Africa: a cautionary tale', Conflict, Security & Development, 10: 2, 263 — 285.

cybernétiques. Dans ce contexte, des allégations non fondées peuvent se propager rapidement.

De nombreuses inexactitudes sur des incidents cybernétiques sont répétées maintes et maintes fois, alors qu'il n'existe souvent pas de preuves tangibles au-delà de simples spéculations. Le président américain Barack Obama, par exemple, a déclaré : «Nous savons que des intrus ont sondé notre réseau électrique et que dans d'autres pays, des cyber-attaques ont plongé des villes entières dans les ténèbres »[17] – mais sans mentionner les pays en question. Les médias américains ont repris cette histoire, et l'émission télévisée populaire *60 Minutes* a affirmé que « plusieurs sources de renseignement fiables avaient confirmé que plusieurs cyber-attaques avaient eu lieu au Brésil » en 2005 et en 2007[18]. Ces allégations continuent d'être répétées par les médias sans aucune justification. Selon un câble de Wikileaks et une déclaration du régulateur de l'électricité brésilien, les pannes n'étaient pas le résultat de cyber-attaques, mais avaient été plutôt causées par « une pollution dans la chaîne des isolateurs due à des dépôts de suie »[19].

Militarisation du cyberespace et course aux cyberarmements

La cybersécurité est de plus en plus intégrée aux programmes de sécurité des États. Les États du monde entier sont en train d'établir au sein de leurs forces armées des « cyber-commandements » ou cyber-unités. La capacité du cyber-commandement américain est opérationnelle depuis mai 2010. Les cyber-commandements intéressent aussi d'autres États. Le secrétaire à la Défense du Royaume-Uni a proposé un cyber-commandement intégré dans le cadre du ministère de la Défense. Le ministère indien de la Défense cherche à établir une autorité de cyber-contrôle et de cyber-commandement. La Chine a mis en place une « Armée bleue » pour défendre l'Armée populaire de libération contre des attaques sur ses réseaux[20]. L'Iran prévoit de créer un cyber-commandement pour ses forces armées[21]. On utilise des cyber-unités pour réprimer les dissidents en ligne[22]. En mars 2011, lors d'une réunion du « cyber-bataillon » du parti au pouvoir du Soudan, le parti a annoncé que les « cyber-djihadistes » « écraseraient » les dissidents en ligne qui appelaient à un changement de régime. Des cyber-unités sont également déployées dans les conflits, par exemple en Syrie, où des partisans du gouvernement ont créé « l'Armée syrienne électronique » qui sert à surveiller les activistes et les membres de l'Armée syrienne libre[23]. « D'autres adoptent des moyens moins conventionnels, notamment un soutien tacite aux groupes patriotiques afin qu'ils lancent des cyber-attaques pour défendre l'État, comme on le voit en Iran, en Syrie, en Russie, en Birmanie et en Chine »[24].

Les États affectent des ressources croissantes à la sécurité de l'information, ainsi qu'à la guerre de l'information. En 2011, alors que les États-Unis se trouvaient en pleine crise budgétaire, le Pentagone a demandé que 3,2 milliards de dollars soient alloués à la cybersécurité, un chiffre à peu près équivalent aux dépenses militaires du Maroc ou de l'Argentine cette année-là[25]. L'augmentation des dépenses militaires consacrées à la guerre cybernétique est certainement un gaspillage de ressources, en plus de n'être pas nécessairement la bonne solution aux problèmes de cybersécurité.

L'internet est de plus en plus militarisé. Les virus, naguère les outils des cybercriminels et de farceurs occasionnels, sont activement développés par des agences militaires et de renseignement. Le virus Stuxnet, responsable du sabotage de centrifugeuses utilisées pour le programme d'enrichissement de l'uranium iranien a été le premier virus largement répandu spécialement conçu pour infecter de l'équipement industriel. Stuxnet a été probablement conçu et déployé avec l'appui des agences de renseignement et de sécurité d'État (prétendument des États-Unis

17. Cyberwar: Sabotaging the System, CBS News, 15 juin 2010, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml voir le segment de 60 Minutes à https://www.youtube.com/watch?v=IPHHd8YW9EA (partie 1) et https://www.youtube.com/watch?v=dU2XPFoyAR8 (part 2).

18. Ibid.

19. Marcello Soares, Brazilian Blackout Traced to Sooty Insulators, Not Hackers, Wired Magazine, 11 novembre 2009, http://www.wired.com/threatlevel/2009/11/brazil_blackout/. Brian Krebs, Cable: No Cyber Attack in Brazilian '09 Blackout, Krebs on Security, 3 décembre 2010, http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout/

20. Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", Peace Magazine 27(4), octobre 2011, http://peacemagazine.org/archive/v27n4p16.htm

21. Iran to launch first cyber command, Press TV, 15 juin 2011, http://presstv.com/detail/184774.html

22. Sudan's NCP says its "cyber-Jihadists" ready to "crush" online oppositionists, Sudan Tribune, March 22 2011, http://www.sudantribune.com/Sudan-s-NCP-says-its-cyber,38372

23. "What is the Syrian Electronic Army?", Mashable, 12 août 2012, http://mashable.com/2012/08/10/syrian-electronic-army/

24. Deibert, op. cit.

25. Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", op. cit.

et d'Israël)[26]. Cofer Black, l'ancien directeur du Centre antiterroriste de la CIA (et directeur d'une filiale de la plus grosse entreprise de sécurité privée travaillant pour le Département d'État américain), a annoncé au Black Hat de 2011, une conférence sur la sécurité de l'information, que Stuxnet était le « Rubicon de notre avenir »[27]. Que cet événement représente ou non un tournant historique (ou une admission implicite de la participation d'une agence américaine à Stuxnet), il met en lumière l'acceptation tacite par le complexe militaro-industriel de l'utilisation des virus par les État dans de futurs conflits de l'information.

Depuis Stuxnet, un autre virus a été signalé, le virus Flame, qui s'est propagé dans un certain nombre de pays au Moyen-Orient et en Afrique du Nord en utilisant le code Stuxnet. Ce code source Stuxnet est désormais disponible sur l'internet, ce qui permet à une multitude d'acteurs de l'adapter à leurs propres fins.

Le ministère de la Défense du Japon a demandé à Fujitsu de développer un « virus défensif » au prix de 2,3 millions de dollars US, qui a « la capacité d'identifier avec une grande précision la source d'une cyber-attaque et de se répliquer d'un ordinateur à l'autre en nettoyant les virus sur le réseau ». Mais selon un expert de la sécurité, le virus « pourrait avoir des conséquences inattendues, notamment être difficile à contrôler ». Un « bon » virus incontrôlé risque de se propager au hasard ou devenir difficile à contenir[28]. S'il se répand hors du Japon, le virus pourrait également atteindre à la souveraineté d'autres pays et éventuellement déclencher un conflit.

Le complexe industriel de la cybersécurité

> *« Dans les conseils du gouvernement, nous devons nous prémunir contre l'acquisition d'une influence injustifiée, qu'elle soit recherchée ou non, par le complexe militaro-industriel. Le potentiel d'une montée désastreuse d'un pouvoir malavisé existe et persistera. Nous ne devons jamais laisser le poids de cette combinaison mettre en danger nos libertés ou nos processus démocratiques. Nous ne devons rien prendre pour acquis. Seuls des citoyens vigilants et informés peuvent assurer le bon fonctionnement de l'énorme machine industrielle et militaire de la défense par nos méthodes et nos buts pacifiques, afin que la sécurité et la liberté puissent prospérer ensemble »*
>
> - Dwight D. Eisenhower, président des États-Unis d'Amérique, Discours d'adieu à la Nation, 1961[29]

L'émergence d'un complexe cyberindustriel représente une autre menace importante en matière de cybersécurité. Les armées modernes ont développé des réseaux d'affaires complexes avec les fournisseurs d'équipements de défense et de services de défense. Le personnel des entreprises de défense sont souvent d'anciens employés du gouvernement : le phénomène de porte tambour. Les deux ont tout intérêt à voir augmenter les budgets de défense et, dans le but de justifier ces budgets, ils ont besoin de présenter des menaces à leurs citoyens, aux parlements et aux gouvernements. Le complexe militaro-industriel est toujours à la recherche de nouvelles menaces pour justifier de nouvelles dépenses, et les nouvelles cyber-menaces leur offre cette possibilité. Le complexe cyber-industriel ne se contente pas de développer des cyber-armes offensives et défensives, il développe également du matériel de surveillance. Une nouvelle industrie est en train de naître qui « secrètement, récupère les données et les préserve pour toujours sur des serveurs de pointe contenant de grandes quantités de pétaoctets (un million de gigaoctets) d'information ». Cette nouvelle industrie « offre de

26. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", Wired, 11 juillet 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/

27 Tabassum Zakaria, "Former CIA official sees terrorism-cyber parallels", Reuters, 3 août 2011, http://www.reuters.com/article/2011/08/03/us-usa-security-cyber-idUSTRE7727AJ20110803; et Glenn Chapman, "Cold War gives way to Code War: CIA veteran", Agence France Presse, 4 août 2011, http://www.google.com/hostednews/afp/article/ALeqM5h-_86Ftav0uDHvMYDzydPgVWjNzQ?docId=CNG.0dcc70d787af82f2b283aeb2af9d940e.e01

28. Gerry Smith, Fujitsu Cyberweapon Developed In Japan: 'Good' Virus Created For Cyber Defense, Huff Post Tech 04, janvier 2012, http://www.huffingtonpost.com/2012/01/04/fujitsu-cyberweapon-japan_n_1183462.html. Voir également Graham Cluley, Why Japan's search-and-destroy cyber weapon could be a very bad idea, Naked Security, 12 janvier 2012, http://nakedsecurity.sophos.com/2012/01/03/japan-cyber-weapon-bad/

29. Texte à : http://coursesa.matrix.msu.edu/~hst306/documents/indust.html, Vidéo à : http://www.youtube.com/watch?v=8y06NSBBRtY

nouveaux outils pour rechercher ces données afin de reconstruire notre passé, voire nos mouvements en temps réel via nos téléphones mobiles, d'une façon qui pourrait bien revenir nous hanter »[30].

CYBERSÉCURITÉ ET CENSURE

La cybersécurité peut servir à introduire et légitimer des modes de censure et les normaliser. En Russie, par exemple, un registre unique de sites Web interdits est destiné à permettre au gouvernement de fermer les sites internet jugés nuisibles pour les enfants, y compris les sites contenant de la pornographie infantile, de l'information sur les drogues et de l'information sur la façon de se suicider. Mais le registre « pourrait conduire à une censure aléatoire de sites Web et de la liberté d'expression »[31] et « finir par bloquer tous les types de discours politiques en ligne » et « grâce à la diffusion des nouvelles technologies de surveillance sur internet, le registre pourrait bien devenir un moyen d'espionner des millions de Russes »[32].

Le rôle des agences de renseignement

Il y a là un conflit d'intérêts fondamental s'agissant de la cybersécurité. Les agences de renseignement tiennent sans doute à sécuriser leurs propres infrastructures, mais si elles veulent surveiller d'autres agences, elles ne veulent pas nécessairement que celles-ci disposent d'infrastructures d'information sécurisées. Il est beaucoup plus difficile de collecter des renseignements sur des canaux de communication sécurisés et privés que sur des infrastructures non sécurisées. Par conséquent, nous devons être sceptiques quand les agences de renseignement font de la cybersécurité et nous devons veiller à ce que leurs activités soient soumises à un contrôle civil et parlementaire. La société civile et les législateurs doivent être particulièrement vigilants à cet égard.

Cybersécurité et surveillance

La cybersécurité devrait viser à protéger les internautes contre la surveillance. Or, les initiatives de cybersécurité peuvent donner aux entreprises et aux gouvernements encore plus de pouvoir pour espionner les utilisateurs. Par exemple, le projet de loi sur la cybersécurité de 2012 déposé aux États-Unis aurait « accordé aux entreprises de nouveaux pouvoirs pour espionner les utilisateurs, communiquer l'information au gouvernement et réclamer une immunité juridique pour leurs actions »[33]. La seconde itération de la Loi sur la communication et la protection des cyber-renseignements, dont la Chambre des représentants des États-Unis est saisie, constituerait une exception en matière de cybersécurité et l'emporterait sur les lois actuelles sur la protection de la vie privée. Les entreprises bénéficieraient d'une large immunité contre la communication de renseignements, y compris les communications privées des utilisateurs avec les organismes gouvernementaux, au nom de la cybersécurité. Les entreprises auraient les coudées franches pour recueillir et communiquer « des renseignements relevant de la cybersécurité », y compris des renseignements personnels, la seule limite étant que les renseignements soient recueillis à des fins de cybersécurité »[34].

Nouvelles menaces pour les médias sociaux

La croissance du complexe cyber-industriel, ainsi que de nos présences en ligne dans les réseaux sociaux et les médias sociaux, a considérablement accru les capacités de surveillance des agences de renseignement. Par exemple, en 2009, l'Agence centrale de renseignement des États-Unis a investi dans une entreprise qui se spécialise dans la surveillance des médias sociaux. L'entreprise, appelée Visible, passe sur plus d'un demi-million de sites Web 2.0 par jour et récupère plus d'un million de messages et de conversations sur les blogues, forums en ligne, Flickr, YouTube, Twitter et Amazon[35].

30. Pratap Chatterjee, The new cyber-industrial complex spying on us, *The Guardian*, 2 décembre 2011, http://www.guardian.co.uk/commentisfree/cifamerica/2011/dec/02/cyber-industrial-complex-spying

31. Bryan Bishop, Internet censorship bill passes upper house of Russian Parliament, The Verge July 18 2012, http://www.theverge.com/2012/7/18/3168011/internet-censorship-bill-passes-upper-house-russian-parliament

32. Andrei Soldatov & Irina Borogan, The Kremlin's New Internet Surveillance Plan Goes Live Today, *Wired*, 1er novembre 1 2012. http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

33. Mark M. Jaycox, The Cybersecurity Act was a surveillance bill in disguise, *The Guardian*, 2 août 2012.

34. Mark M. Jaycox, CISPA, the Privacy-Invading Cybersecurity Spying Bill, is Back in Congress, Electronic Frontier Foundation, 13 février 2013, https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cybersecurity-spying-bill-back-congress

35. Noah Schachtman, U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets, *Wired Magazine*, 19 octobre 2009, http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

En plus du risque d'exposer la société civile à la surveillance, les médias sociaux peuvent aussi l'exposer à la manipulation. Les entreprises de cybersécurité ont développé un logiciel qui crée de faux personnages sur les réseaux sociaux à des fins de surveillance et pour manipuler les conversations en ligne en imitant l'apparence de mouvements locaux, une pratique appelée « astroturfing ». Par exemple, en 2010, l'US Air Force a sollicité des propositions pour le développement de logiciels d'astroturfing - ou « gestion des personnages virtuels » - qui permettraient le contrôle des faux personnages sur les plateformes de médias sociaux[36].

Le logiciel Astroturfing serait un outil de surveillance et de propagande, en faisant croire que l'information vient légitimement de la société civile. Il s'agit d'une menace grave pour la sécurité de l'information (la sécurité de l'information telle qu'elle est mentionnée ci-dessus vise à protéger la «confidentialité, l'intégrité et la disponibilité » de l'information et des communications.) Le journaliste George Monbiot a déclaré que « les logiciels comme celui-ci risquent de détruire l'internet comme lieu de débat constructif. C'est se moquer de la démocratie en ligne »[37].

Sécurité des logiciels : *Jours zéro* et *jours infinis*

Les articles sur la cybersécurité sont généralement passionnants (ou terrifiants). Mais le véritable défi de la cybersécurité n'a rien à voir avec le terrorisme international, l'espionnage d'État ou les pirates dopés aux stéroïdes. Le problème réside dans le code source du logiciel que nous utilisons tous les jours, que ce soit les systèmes d'exploitation, les « apps » que nous exécutons sur nos ordinateurs, nos navigateurs Web et les modules complémentaires qui les exécutent (p. ex. Flash et Java) et le logiciel utilisé pour créer les sites Web qui peuplent l'internet. Le vrai problème de la cybersécurité réside dans la *sécurité des logiciels*. Il est généralement admis que l'internet (le protocole TCP/IP) et le web n'ont pas été conçus pour être sécurisés. L'internet était à l'origine un réseau universitaire de pairs qui se faisaient confiance. Les problèmes de confiance et de sécurité n'étaient pas importants à cette époque et n'avaient pas été spécialement abordés. Malgré les progrès réalisés dans les infrastructures de sécurisation (développement des extensions de sécurité du système de noms de domaine (DNSSEC)[38] et le protocole HTTPS[39] par exemple), il est généralement admis que l'internet ne peut pas être refondu pour tenir compte de la sécurité et que cette refonte poserait des problèmes d'interopérabilité. Au sommet de la couche des infrastructures de l'internet ouvert se trouve la couche des applications. Ce sont les applications qui existent localement sur nos ordinateurs, dans le logiciel qui facilite l'accès aux services web et internet, comme les navigateurs, les messages instantanés et le VoIP (p. ex., Skype), et le logiciel qui entraîne les services en ligne et les sites web sur lesquels nous stockons nos données. C'est dans cette couche que la sécurité peut être intégrée, mais c'est aussi dans cette couche où l'insécurité est la plus grande. C'est aussi dans cette couche que nous pouvons installer le plus facilement des correcteurs qui assurent la sécurité de nos informations.

L'expertise dans la correction des bugs de sécurité dans le code s'améliore, mais sans suivre le rythme de croissance des nouveaux bugs. Par rapport à il y a 15 ans, tous les systèmes d'exploitation de bureau populaires et contemporains (Windows, Linux et Mac) proposent régulièrement des mises à jour de sécurité automatiques pour découvrir les bugs de sécurité qui sont ensuite réparés par les mises à jour. Même s'il y a plus de bugs et de virus que jamais, on les découvre aussi de plus en plus facilement. En même temps, on continue de produire de plus en plus de code (applications d'ordinateur et en ligne) de sorte que le nombre net de bugs, et donc

36. John Hudson, The Embarrassing Revelations of Cyber Security Firm HBGary Federal, The Atlantic Wire, 24 février 2011, http://www.theatlanticwire.com/technology/2011/02/the-embarrassing-revelations-of-cyber-security-firm-hbgary-federal/20977; Happy Rockefeller, The HB Gary Email That Should Concern Us All, The Daily Kos, 16 février 2011, http://www.dailykos.com/story/2011/02/16/945768/-UPDATED-The-HB-Gary-Email-That-Should-Concern-Us-All, La demande de propositions originale "Persona Management Software" (Solicitation number: RTB220610 22 June 2010) visait un service de gestion des personnages en ligne. 50 licences d'utilisateur, 10 personnages par utilisateur. Le logiciel prévoit 10 personnages par utilisateur, avec contexte historique, détails justificatifs et présences en ligne qui sont techniquement, culturellement et géographiquement cohérents. Les applications permettront à un opérateur d'avoir un certain nombre de personnes en ligne à partir du même poste de travail et sans crainte d'être découverts par des adversaires avertis. Les personnages doivent pouvoir donner l'impression de venir de n'importe quelle partie du monde et communiquer dans le cadre de services en ligne conventionnels et plateformes de médias sociaux. Le service comprend un environnement d'applications conviviale pour maximiser la connaissance situationnelle de l'utilisateur en affichant de l'information locale en temps réel », première parution à FedBizOpps.gov, archivée à : http://www.seankerrigan.com/docs/PersonaManagementSoftware.pdf

37. Ibid.

38. Les DNSSEC sont un ensemble de spécifications du Internet Engineering Task force qui ajoutent des extensions au service DNS qui apportent une authentification d'origine des données et l'intégrité des données au système des noms de domaine. Mais il n'assure pas la confidentialité.(Voir Arends, et al., Request For Comment 4033, DNS Security Introduction and Requirements, mars 2005. Internet Engineering Task Force, http://tools.ietf.org/html///rfc4033; Voir également RFCs 4034, and 4035, and http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions pour une bonne explication.

39. The Hypertext Transfer Protocol Secure (HTTPS) ajoute une certaine sécurité par le the Hypertext Transfer Protocol (HTTP) en ajoutant un cryptage bidirectionnel entre l'utilisateur et le site web (http://en.wikipedia.org/wiki/HTTP_Secure).

des failles de sécurité dans notre code augmente, d'où encore plus de bugs que jamais[40].

Un bug de sécurité (également appelé vulnérabilité) est essentiellement un morceau de code logiciel non sécurisé qui peut donc être exploité pour avoir accès à des données auxquelles on ne devrait pas avoir accès dans des circonstances normales. Lorsqu'un bug est découvert, un pirate peut faire un « exploit » pour compromettre des données ou accéder à un ordinateur. Les logiciels malveillants - virus et chevaux de Troie – sont des exploits qui tirent parti de ces bugs. Il existe deux grands types de bugs logiciels qui sont très pertinents pour la cybersécurité, et leur traitement est probablement le moyen le plus efficace de sécuriser le cyberespace : ce sont les jours zéro et les jours infinis.

Les jours zéro sont des bugs ou vulnérabilités qui ont été découverts, à l'insu des développeurs du logiciel original. Les fournisseurs du logiciel ne parviennent pas à le réparer, soit parce qu'ils ne sont pas au courant de l'existence du bug, soit parce qu'ils n'ont pas eu le temps de réparer. Ils ont eu un « jour zéro » pour corriger la vulnérabilité. Une attaque de jour zéro est une attaque qui tire parti d'une vulnérabilité de jour zéro. Elles sont particulièrement dangereuses, la plupart des gens, autres que les chercheurs en sécurité ou ceux qui ont une intention malveillante, n'étant pas conscients de la vulnérabilité et étant donc incapables de se protéger Les attaques de cybersécurité les plus graves proviennent de bugs et d'exploits jour zéro. Lorsque l'on trouve un jour zéro, il faut informer le développeur du logiciel d'origine pour qu'il trouve un correctif. On doit également informer, à un moment donné, les utilisateurs du logiciel concernés qui sont rendus vulnérables, et éventuellement d'autres parties prenantes et la population en général. « Comme la plupart des technologies, les exploits ont un double usage : on les utilise dans le cadre de la recherche visant à renforcer les ordinateurs contre les intrusions, mais aussi comme arme déployée de façon agressive pour tout, de l'espionnage d'État à l'espionnage commercial en passant par la fraude »[41]. « Un récent article de Forbes, souligne la croissance du marché des jours zéro qui opère d'une manière floue et non réglementée. « Certaines entreprises légitimes opèrent dans une zone grise juridique sur le marché des jours zéro en vendant des exploits aux gouvernements et aux organismes d'application de la loi dans le monde entier... Mais du fait que les ventes ne sont pas réglementées, il est à craindre que certaines entreprises du marché gris approvisionnent des régimes voyous susceptibles de se servir des exploits pour mener des attaques malveillantes qui ciblent d'autres pays ou des opposants. Il existe également un marché noir anarchique... où les exploits sont vendus à n'importe qui, souvent à des fins criminelles » et « il est à craindre que le commerce en plein essor de la recherche et de la vente d'exploits ne devienne incontrôlable, d'où la demande de nouvelles lois pour freiner ce commerce trouble »[42]. Il est important d'envisager une réglementation concernant les jours zéro. On doit encourager les éditeurs de logiciels à trouver et à corriger les jours zéro dans leurs propres logiciels; on doit également inciter les chercheurs en sécurité à trouver les jours zéro et à informer les entreprises et les autres parties prenantes[43].

Un grave problème de cybersécurité pour l'utilisateur moyen, ainsi que pour les infrastructures critiques liées à l'internet, sont les « jours infinis ». Il s'agit de bugs qui ne sont jamais réparés ou prennent un certain temps à l'être, même quand ils sont reconnus par la compagnie qui a développé le logiciel ». Bien que ces bugs touchent éventuellement les internautes ordinaires, ils peuvent toucher des infrastructures essentielles, telles que les systèmes de contrôle industriels, souvent utilisés pour contrôler les infrastructures comme les réseaux électriques. Les systèmes de contrôle industriels ont besoin d'importants investissements dans des équipements censés durer des années. Contrairement au cycle de développement des logiciels, les opérateurs de systèmes de contrôle industriels n'ont pas toujours les moyens de mettre à jour régulièrement leurs systèmes. Il existe par exemple des vulnérabilités bien documentées (« les jours infinis ») dans les systèmes de contrôle Siemens qui ont laissé le virus Stuxnet infecter les réacteurs nucléaires de Natanz en Iran. On se sert également de ces systèmes de contrôle pour une vaste gamme de machines dans différentes applications dans le monde entier, « utilisées dans des centrales nucléaires et d'autres infrastructures critiques, ainsi que dans des usines de fabrication commerciale qui font tout, des produits pharmaceutiques à l'automobile »[44].

40. Gary McGraw, Cyber War, Cyber Peace, Stones, and Glass Houses, talk at Institute for Security, Technology, and Society (ISTS), Dartmouth College, 26 avril 2012, http://www.ists.dartmouth.edu/events/abstract-mcgraw.html, http://www.youtube.com/watch?v=LCULzMa7iqs

41. Ryan Gallagher, Cyberwar's gray market, Slate, 16 janvier 2013, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html; Voir également, Andy Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees), Forbes, 21 mars 2012, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

42. Ryan Gallagher, Cyberwar's gray market, op. cit.

43. Une proposition visant un règlement de ce genre est expliquée dans Sandro Gaycken & Felix FX Lindner, Zero-Day Governance: an (inexpensive) solution to the cybersecurity problem, document présenté à Cyber Dialogue 2012: What is stewardship in cyberspace?, mars 2012, http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf

44. Kim Zetter, Serious security holes found in Siemens control systems targeted by Stuxnet, Ars Technica 4 août 2011, http://arstechnica.com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/

APPROCHE DE LA SOCIÉTÉ CIVILE

Quel devrait être le programme et la stratégie de cybersécurité pour la société civile?

La société civile n'est pas une entité homogène, elle est culturellement diversifiée, aborde un large éventail d'enjeux et comprend un vaste éventail d'opinions divergentes sur la manière d'aborder ces enjeux. Il existe une convergence d'intérêts au sein de la société civile mondiale concernant certains sujets, alors que pour d'autres, il y a divergence d'intérêts. Mais en matière de cybersécurité, la société civile est confrontée à des problèmes communs.

Alors que la société civile devrait généralement favoriser un internet ouvert qui promeut la liberté d'expression et d'accès à l'information, elle a tout intérêt à ce que les communications soient sécurisées. La confiance dans la sécurité et la confidentialité des infrastructures de communication permet à la société civile de mener ses affaires sans se soucier de vol d'argent ou d'informations ni s'inquiéter de surveillance électronique.

Parfois, les mesures visant la sécurité, l'ouverture et la protection de la vie sont incompatibles. Il est essentiel que les initiatives de cybersécurité protègent la capacité d'utiliser l'internet pour exercer les droits à la liberté d'expression et la liberté d'association. Les moyens de sécurisation des réseaux ne devraient pas non plus rendre vulnérable à une surveillance indue et illégale et doivent respecter le droit à la vie privée. La société civile doit aborder la cybersécurité de façon à concilier les préoccupations liées à ces différents droits.

L'approche à l'égard de la cybersécurité fondée sur les droits humains doit concerner la sécurité non seulement des réseaux des États et des gouvernements, mais également celle des réseaux d'entreprises, des réseaux de la société civile et des réseaux des organisations. La sécurité des utilisateurs individuels (les internautes) doit également être au centre de la stratégie de cybersécurité.

La société civile doit être attentive à décider si elle doit introduire certaines questions dans le champ des programmes nationaux de cybersécurité et si oui ou non ces questions y seront mieux traitées. La société civile doit prendre en considération les coûts et les avantages de la titrisation de certaines questions. Revêtent-elles une importance qui justifie de relever de la sécurité nationale? Sont-elles mieux abordées si elles relèvent de la sécurité nationale ou de la sécurité de l'information? Sont-elles actuellement traitées par d'autres structures gouvernementales? Existe-t-il des mécanismes ou des initiatives non liés à l'internet qui en sont déjà saisis? La société civile doit soigneusement réfléchir pour savoir quand titriser des questions et quand ne pas le faire. La titrisation va-t-elle améliorer ou marginaliser le rôle actuel de la société civile? Certaines questions n'ont pas nécessairement besoin d'être titrisées, d'autres peuvent avoir besoin d'être débattues et intégrées au programme de cybersécurité, sans être titrisées, d'autres encore peuvent avoir besoin d'être détitrisées.

On doit encourager les débats multipartites au sujet des stratégies nationales de cybersécurité. La société civile doit participer activement et exiger la présence des parties prenantes au moment de la formulation des politiques et des accords nationaux, régionaux et internationaux sur la cybersécurité. La société civile, les milieux universitaires et techniques, les internautes et les créateurs de contenus (les citoyens du Net), le secteur privé, les entreprises, les militaires et les services de renseignement doivent tous participer aux débats. Les débats multilatéraux sur la cybersécurité doivent être encouragés dans les forums multilatéraux, comme le FGI.

La gouvernance de la cybersécurité doit être abordée de manière à ne pas remplacer d'autres questions de gouvernance d'Internet. Les mécanismes décisionnels actuels sur la gouvernance de l'internet aux niveaux national et international ne doivent pas être remplacés par d'autres mécanismes décisionnels qui seraient exclusivement axés sur la cybersécurité.

Les politiques sur la cybersécurité doivent renforcer la sécurité des femmes défenseurs des droits humains et veiller à ce que les stratégies de sécurité nationale traitent de la violence faite aux femmes, en ligne et hors ligne[45]. Les femmes défenseurs des droits humains doivent également renforcer leurs capacités en ce qui concerne d'importants outils technologiques pour protéger leur sécurité opérationnelle et physique, notamment le cryptage ou les outils d'anonymat.

Enfin, la société civile doit exiger la tenue de débats fondés sur les faits en matière de cybersécurité. En raison du problème de l'attribution dans ce domaine, il est facile de prendre des décisions en s'appuyant sur des faits inexacts. Les demandes que font les décideurs qui invoquent des incidents et des menaces cybernétiques doivent être étayées par des preuves.

45. Voir également Danna Ingleton, "Let's stop our fear of tech leading to misuse of security legislation" GenderIT, 25 octobre 2012, http://www.genderit.org.

ASSOCIATION
POUR LE PROGRÈS DES
COMMUNICATIONS

UN PLAN DE CYBERSÉCURITÉ POUR LA SOCIÉTÉ CIVILE : LES ENJEUXLES ENJEUX

APC est un réseau international d'organisations de la société civile. Fondé en 1990, sa mission consiste à autonomiser et appuyer des personnes qui œuvrent pour la paix, les droits humains, le développement et la protection de l'environnement, par l'utilisation stratégique des technologies de l'information et de la communication (TIC).

APC travaille à la construction d'un monde dans lequel toute personne jouit d'un accès facile, équitable et abordable au potentiel créateur des TIC afin d'améliorer sa vie et d'oeuvrer à la création de sociétés plus démocratiques et égalitaires.

www.apc.org info@apc.org

Conception graphique: MONOCROMO

Commandé par l'Association pour le progrès des communications (APC)

Conduit avec le soutien de L'Agence suédoise pour la coopération et le développement international (Sida).

BRANCHEZ VOS DROITS!

UN PLAN DE CYBERSÉCURITÉ POUR
LA SOCIÉTÉ CIVILE : LES ENJEUX
Avril 2013

APC-201304-CIPP-R-FR-DIGITAL-185

ISBN : 978-92-95096-94-3